Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 2 (2010) 227–235
Procedia Computer Science
www.elsevier.com/locate/procedia
ICEBT 2010

Biometric Template Security based on Watermarking

Gaurav Bhatnagar*, Q.M. Jonathan Wu, Balasubramanian Raman

[1,2]*Department of Electrical and Computer Engineering, University of Windsor, Windsor, Ontario, ON, N9B 3P4, CANADA*
[3]*Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee-247 667, INDIA*

Abstract

This paper presents a secure and robust watermarking scheme to enhance the security of biometric template over insecure network. Diffusion and digital watermarking techniques are used to improve the security and secrecy of the templates. Diffusion phase is done by chaotic sequence and Hessenberg decomposition. This phase essentially change the pixel values of biometric template randomly. Finally, the watermark image, which is the face image of the owner of biometric template, is embedded in the diffused biometric template with the help of singular value decomposition. The feasibility of the proposed method and its robustness against different kind of attacks are verified by computer simulations.

Keywords: Biometrics, Hessenberg Decomposition, Singular Value Decomposition, Chaotic Map.

1. Introduction

Nowadays, biometric recognition is a well-known research area that aims to provide more efficient solutions to the ever-growing human need for security. Biometrics [1] refers to one or more intrinsic physical or behavioral characteristics which uniquely identify individuals. This identification of individuals is done through one-to-many matching across large shared database which further provide a convenient authentication services for many applications including information security, physical access, financial services etc. But the multiple uses of biometric databases raises a serious issue with respect to personal privacy because biometric template having personal information could be used for unauthorized purposed. Unlike a PIN or password, a biometric template cannot be changed, recovered, or reissued if it is hacked or misused. By their nature, biometric entities are stable over time otherwise their utility would be quite limited.

One potential means of protecting stored biometric templates is encryption [2, 3]. Since, every biometric recognition method is used to match templates and thereby individual identity authentication cannot be done on such encrypted templates, the templates must be decrypted prior to matching. Furthermore, encryption can be computationally expensive and limit the capacity of large-scale biometric systems to provide responsive authentication services. Hence, watermarking [4, 5, 6, 7] comes into picture and is used to achieve the biometric data security and secrecy [8, 9]. Some schemes related with watermarking and steganography are proposed for the biometric data security [10, 11, 12, 13, 14]. To improve the security and secrecy, this paper presents a novel semi-blind watermarking

*Corresponding author: Email address: goravb@uwindsor.ca (Gaurav Bhatnagar)

1877-0509
doi:10.1016/j.procs.2010.11.029

scheme for biometric templates. For this purpose, the biometric template is first defused using non-linear chaotic map and Hessenberg decomposition. Diffusion essentially changes the pixels values of biometric template randomly. Hessenberg decomposition is used to ensure the perfect inverse diffusion. After that the watermark which is the face image of the person whose biometric template has to be secure is embedded in the singular values of the diffused image. The main benefit of proposed scheme is that the initial conditions for non-linear chaotic map is used as the keys since chaotic trajectory is sensitive to its initial conditions. Another benefit is that all existing schemes using SVD need original image and singular vectors in order to extract watermark whereas in the proposed scheme one key image is required instead of original image and singular vectors. The experimental results demonstrate the robustness and superiority of the proposed scheme.

The rest of paper is organized as follows: In section 2, mathematical preliminaries are illustrated followed by the proposed security framework for biometric templates in sections 3. In section 4, experimental results using proposed framework are presented and finally section 5 gives the concluding remarks regarding proposed security framework.

2. Mathematical Preliminaries

This section reviews the basic mathematical concepts and results which are used in the proposed watermarking scheme for biometric templates. These concepts are as follows.

2.1. Non-linear Chaotic Map

A chaotic system is a deterministic non-linear system with pseudo stochastic property [15]. Due to its interesting properties like non-periodicity, unpredictability, initial parameter sensitivity and Gauss like statistical characteristics, many chaotic systems serve as the stochastic signal/sequence generator nowadays. In this work, we have used piecewise non-linear map in order to create digital sequence. Mathematically, a piecewise non-linear map (PWNLM) $\mathcal{F} : I \to I$ where $I = [0,\ 1]$ and also denote the length of the region, described as [16]

$$\mathcal{F}(x_{k+1}) = \begin{cases} \left(\dfrac{1}{I_{i+1} - I_i} + a_i\right)(x_k - a_i) - \dfrac{a_i}{I_{i+1} - I_i}(x_k - a_i)^2, & \text{if } x_k \in [I_i, I_{i+1}) \\ 0, & \text{if } x_k = 0.5 \\ \mathcal{F}(x_k - 0.05), & \text{if } x_k \in (0.5, 1] \end{cases} \tag{1}$$

where $x_k \in [0, 1]$ and I_i is the sub-interval of [0,1] such that $0 = I_0 < I_1 < \cdots < I_i < \cdots < I_{n+1} = 0.5$. The parameter $a_i \in (-1, 0) \cup (0, 1)$ tune sequence in the i^{th} interval such that

$$\sum_{i=0}^{n-1} (I_{i+1} - I_i)a_i = 0 \tag{2}$$

The interesting properties of the above mentioned map are summarized as follows.

- The iteration system obtained by Eqn. 1 i.e. $x_{k+1} = \mathcal{F}(x_k)$ is chaotic for all $x_k \in [0, 1]$.
- The sequence $\{x_k\}_{k=1}^{\infty}$ is ergodic in [0,1] having the uniform probability distribution function $\varrho(x) = 1$, which further shows the uniformity of the map i.e the probability of each value in [0,1] is equal to be selected.
- The sequence $\{x_k\}_{k=1}^{\infty}$ has δ-like autocorrelation function given as

$$R_{\mathcal{F}}(r) = \lim_{j \to \infty} \frac{1}{j} \frac{\sum_{k=1}^{j} x_k x_{k+r}}{\sum_{k=1}^{j} x_k^2}, r \geq 0$$

2.2. Singular Value Decomposition

Singular value decomposition is a linear algebraic scheme, which is developed for a variety of applications. This transform was introduced for square matrices by Beltrami in 1873 and Jordan in 1874, and was extended for rectangular matrices by Eckart and Young in 1930. Let A be a general real(complex) matrix of order $m \times n$. The singular value decomposition (SVD) of A is the factorization [17]:

$$A = U * S * V^T \tag{3}$$

where U and V are *orthogonal (unitary) matrices* and S is a *diagonal matrix* given by $S = diag(\sigma_1, \sigma_2, ..., \sigma_r)$, where σ_i, $i = 1(1)r$ are the singular values of the matrix A with $r = min(m, n)$ and satisfying $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r$. The first r columns of V are called *right singular vectors* and the first r columns of U are called *left singular vectors*.

Use of SVD in digital image processing has some advantages. Singular values possess the algebraic and geometric invariance to some extent. The properties of the singular values are summarized as follows

- The size of the matrices from SVD transformation is not fixed. It can be a square or a rectangle.
- *Scaling*: given an image I and its scale I^s, if I has the singular values σ_i, then I^s has the singular values $\sigma_i * \sqrt{L_R L_C}$ where L_R and L_C are the scaling factors along rows and columns respectively. If rows (columns) are mutually scaled, I^s has the singular values $\sigma_i * \sqrt{L_R}(\sigma_i * \sqrt{L_C})$.
- *Translation*: given an image I and its translated I^t, both have the same singular values.
- *Rotation*: given an image I and its rotated I^r, both have the same singular values.
- *Transpose*: given an image I and its transpose I^T, both have the same singular values since,

$$\text{if } AA^T\ U = \sigma\ U \text{ then } A^T A\ V = \sigma\ V \tag{4}$$

2.3. Hessenberg Decomposition

Hessenberg Decomposition [17] is the factorization of a general matrix A by orthogonal similarity transformations into the form

$$A = QHQ^T \tag{5}$$

where Q is an orthogonal and H is an upper Hessenberg matrix, meaning is that $h_{ij} = 0$ when ever $i > j + 1$ i.e.

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1(n-1)} & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2(n-1)} & h_{2n} \\ 0 & h_{32} & \cdots & h_{3(n-1)} & h_{3n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & h_{n(n-1)} & h_{nn} \end{bmatrix} \tag{6}$$

Hessenberg decomposition is typically computed using Householder matrices. Householder matrix (P) is the orthogonal matrices of the form

$$P = I_n - 2uu^T / u^T u$$

where u is a non-zero vector in R^n and I_n is the $n \times n$ identity matrix. The main reason of using these matrices is the ability of introducing zeros. For instance, suppose $x = (x_1, x_2, ..., x_n)$ is a non-zero vector in R^n and u is defined as

$$u = x + sign(x_1)\|x\|_2 e_1$$

where $sign(x_1) = \dfrac{x_1}{|x_1|}$ and e_1 is the first column of I_n. It then follows that

$$Px = -sgn(x_1)\|x\|_2 e_1$$

i.e. a vector having zeros in all but its first component. There are $n-2$ steps in the overall procedure when A is of size $n \times n$ which is further proves the ability of introducing zeros. At the beginning of k^{th} step orthogonal matrices $P_1, P_2, ..., P_{k-1}$ have been expressed as

$$A_{k-1} = (P_1 P_2 ... P_{k-1})^T A (P_1 P_2 ... P_{k-1}) \tag{7}$$

having the form

$$A_{k-1} = \begin{matrix} \\ k-1 \\ 1 \\ n-k \end{matrix} \begin{matrix} \begin{matrix} k-1 & 1 & n-k \end{matrix} \\ \begin{bmatrix} H_{11}^{(k-1)} & H_{12}^{(k-1)} & H_{13}^{(k-1)} \\ 0 & b_{22}^{k-1} & H_{23}^{(k-1)} \\ 0 & H_{32}^{(k-1)} & H_{33}^{(k-1)} \end{bmatrix} \end{matrix} \tag{8}$$

where $H_{11}^{(k-1)}$ is Hessenberg matrix. Let

$$\widetilde{P}_k = I_{n-k} - 2u^k \left(u^k\right)^T / \left(u^k\right)^T u^k$$

be a Householder matrix with the property that $\widetilde{P}_k b^{k-1}$ has zeros in the last $n-j-1$ components which further follows that the matrix $P_k = diag(I_{n-k}, \widetilde{P}_k)$ is orthogonal and A_k is given as

$$A_k = P_k^T A_{k-1} P_k = (P_1 P_2 ... P_{k-1} P_k)^T A (P_1 P_2 ... P_{k-1} P_k) = \begin{matrix} \\ k \\ 1 \\ n-k-1 \end{matrix} \begin{matrix} \begin{matrix} k & 1 & n-k-1 \end{matrix} \\ \begin{bmatrix} H_{11}^{(k-1)} & H_{12}^{(k-1)} & \left(H_{13}^{(k-1)}\right)^T \widetilde{P}_k \\ 0 & b_{22}^{k-1} & \left(H_{23}^{(k-1)}\right)^T \widetilde{P}_k \\ 0 & \widetilde{P}_k \left(H_{32}^{(k-1)}\right)^T & \widetilde{P}_k H_{33}^{(k-1)\widetilde{P}_k} \end{bmatrix} \end{matrix} \tag{9}$$

where A_k is Hessenberg matrix. Since, we need $n-2$ steps in the over all procedure, the above Eqn. 9 can be rewritten as

$$H = Q^T A Q \Longrightarrow A = QHQ^T \tag{10}$$

where $H = A_{n-2}$ and $Q = P_1 P_2 ... P_{n-3} P_{n-2}$.

3. Proposed Watermarking Scheme for Biometrics

In this section, we discuss some motivating factors in design of our approach to watermarking for biometrics. The proposed embedding method consists of two phases. In the first phase, the original biometric image is altered by the means of chaos and Hessenberg decomposition followed by the embedding in the second phase. Embedding is done by the means of singular value decomposition. The initial watermark used for embedding is a gray scale image, which is either equal or small in size compared to the host image.

Without loss of generality, assume that F represents the host image of size $M \times N$, W represents the watermark of size $m \times n$ and watermark is smaller than the host image by a factor 2^{Q_1} and 2^{Q_2} along both the direction, where Q_1 and Q_2 are any integers greater than or equal to 1. Block diagram of the proposed method is shown in figure 1 and can be summarized as follows.

3.1. Watermark Embedding Process

The goal of embedding process is to embed watermark in the biometric image. The embedding process is formulated as follows:

Step 1: *First Phase:* Adopting K_1 and K_2 as keys iterate non-linear chaotic map to get two sequences of length M^2 and N^2.

Step 2: Stack these sequences in two arrays of size $M \times M$ and $N \times N$ respectively which are denoted by $\mathcal{K}_1$ and $\mathcal{K}_2$.

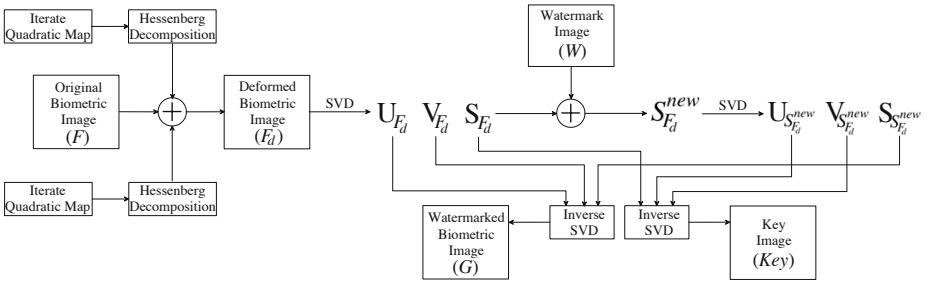

Figure 1: Block Diagram of Proposed Watermarking Scheme.

Step 3: Perform Hessenberg decomposition on $\mathcal{K}_1$ and $\mathcal{K}_2$ to get two orthogonal matrices U_1 and U_2 i.e.

$$\mathcal{K}_1 = Q_1^T H_1 Q_1, \quad \mathcal{K}_2 = Q_2^T H_2 Q_2 \tag{11}$$

Step 4: Diffuse the original biometric image using orthogonal matrices Q_1 and Q_2 as

$$F_d = Q_1 F Q_2^T \tag{12}$$

Step 5: *Second Phase:* Perform SVD transform on diffused biometric image (F_d) as

$$F_d = U_{F_d}\, S_{F_d}\, V_{F_d}^T \tag{13}$$

Step 6: Modify the singular values of diffused image with the help of singular values of the watermark as:

$$S_{F_d}^{new} = S_{F_d} + \alpha\, W \tag{14}$$

where α gives the watermark strength for diffused image.

Step 7: Perform SVD on modified matrix of singular values i.e.

$$S_{F_d}^{new} = U_{S_{F_d}^{new}}\, S_{S_{F_d}^{new}} \left(V_{S_{F_d}^{new}}\right)^T \tag{15}$$

Step 8: Apply inverse SVD to get diffused watermarked and key image i.e.

$$F_d^w = U_{F_d}\ S_{S_{F_d}^{new}}\, V_{F_d}^T, \quad key = U_{S_{F_d}^{new}}\, S_{F_d} \left(V_{S_{F_d}^{new}}\right)^T \tag{16}$$

Step 9: Apply inverse diffusion to get watermarked image (G) i.e.

$$G = inv(Q_1)\ F_d^w\ inv\left(Q_2^T\right) = Q_1^T F_d^w Q_2, \quad \because Q_1 \text{ and } Q_2 \text{ are orthogonal.} \tag{17}$$

3.2. Watermark Extraction Process

The objective of the watermark extraction is to obtain the estimate of the original watermark. For watermark extraction, keys K_1, K_2, watermarked biometric and key image are required. This extraction does not require host image hence it is called as *semi-blind*. The complete process consists of two phases. In first phase, watermarked diffused image is formed with the help of non-linear chaotic map followed by the extraction of watermark in the second phase. The extraction process is formulated as follows:

Step 1: *First Phase:* Adopting K_1 and K_2 as keys and using **step 1** to **step 4**, obtain watermarked diffused image (G_d) as

$$G_d = Q_1 G Q_2^T \tag{18}$$

Step 2: *Second Phase:* Perform SVD transform on diffused watermarked and key images respectively i.e.

$$G_d = U_{G_d} S_{G_d} V_{G_d}^T, \quad key = U_{key} S_{key} V_{key}^T \tag{19}$$

Step 3: Extract the watermark as

$$W^{ext} = \frac{U_{key} S_{G_d} V_{key}^T - S_{key}}{\alpha} \tag{20}$$

4. Experimental Results

In order to explore the performance of proposed biometric template security framework, MATLAB platform is used and a number of experiments are performed on different biometric templates. Here, the results for fingerprint template are given. The fingerprint template is selected because fingerprints are oldest and widely used biometric templates. The biometric template used in experimental results is a grayscale image and is randomly selected from FVC 2002 fingerprint database (FVC-DB1-B) [18] which is of size 388×374. For watermark, 8-bit gray scale image, having the same size as original fingerprint image, is used containing face of the concern person. Since the name of person in FVC-DB1-B is not mentioned, the authors have used their face images. In order to make chaotic sequences, the values for keys i.e. initial conditions are taken to be $K_1 = 0.1576$ and $K_2 = 0.8147$ respectively. In figure 2, original biometric template, original watermark, watermarked biometric template and extracted watermark image are shown. If original and watermarked images are observed then no perceptual degradation is found according to the human visual system. For this purpose, the quality of watermarked fingerprint image is measured using PSNR (Peak Signal to Noise Ratio) which comes out to be 42.5376 dB. Now, the watermarked fingerprint image undergoes to different kinds of intentional and un-intentional attacks, which may occur during the communication and transmission of biometric template, followed by the watermark extraction. In order to verify the quality of extracted watermark, different measures can be used to show the similarity between the original and the extracted watermarks. In the proposed algorithm, used correlation coefficient is given by:

$$\rho(w, \bar{w}) = \frac{\sum_{i,j} [w(i) - w_{mean}][\overline{w}(i) - \overline{w}_{mean}]}{\sqrt{\sum_{i,j} [w(i) - w_{mean}]^2 \sum_{i,j} [\overline{w}(i) - \overline{w}_{mean}]^2}} \tag{21}$$

where w and $\bar{w}$ are the original and the extracted watermark images. The value of ρ lies between [-1, 1]. If the value of ρ is equal to 1 then the singular values of extracted watermark are just equal to the original one. If the value of ρ is -1 then the difference is negative for the largest singular values. In this case, the lighter parts of the image become darker and darker parts become lighter i.e constructed watermark looks like negative thin film. According to statistics, the

(a) (b) (c) (d) (e)

Figure 2: a) Original Fingerprint Image b) Defused Fingerprint Image c) Watermark Image d) Watermarked Fingerprint Image e) Extracted Watermark Image.

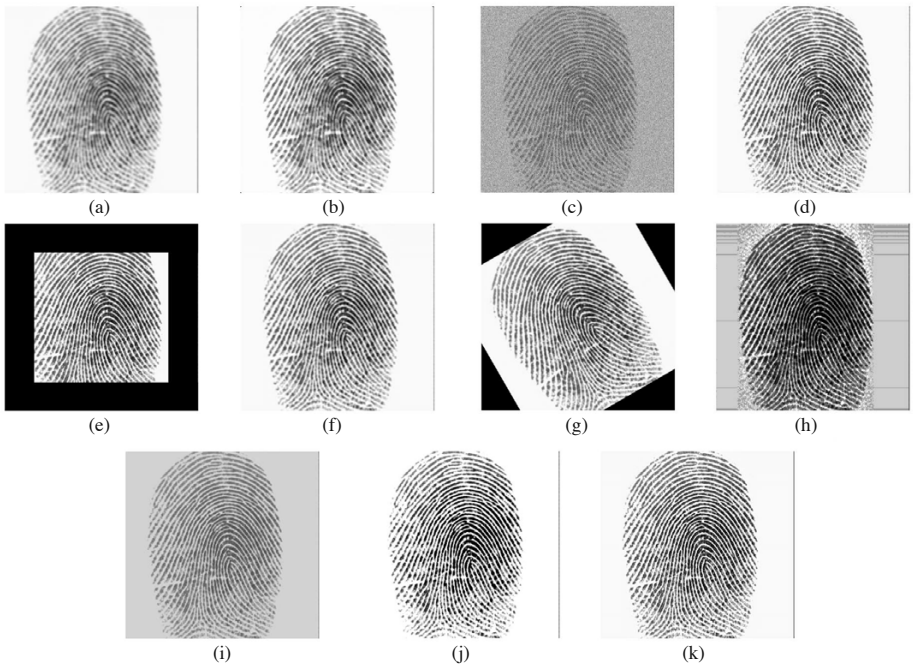

Figure 3: Attacked Watermarked Fingerprint Template with a) Average Filtering (5×5) b) Median Filtering (5×5) c) Gaussian Noise Addition (25%) d) JPEG Compression (CR=50) e) Cropping (60% area remaining) f) Resizing ($388 \times 374 \rightarrow 256 \times 256 \rightarrow 388 \times 374$) g) Rotation ($30^{\circ}$) h) Histogram Equalization i) Contrast Adjustment (Reduced by 50%) j) Contrast Adjustment (Increase by 50%) k) Sharpening (Increase by 50%).

principle range for correlation coefficient is [0, 1]. Hence, the Negative Image Transform (NIT) is performed on the extracted watermark whenever ρ takes negative value, in order to get ρ in the principle range. The NIT with intensity levels in the range [0, L-1] is given by the expression $s = L - 1 - r$, where r is the original intensity and s is the transformed intensity.

To investigate the robustness of the proposed framework, the watermarked fingerprint image is attacked by Average and Median Filtering, Gaussian noise addition, JPEG compression, Cropping, Resizing, Rotation, Histogram Equalization, Contrast adjustment and sharpening attacks. After these attacks on the watermarked image, the extracted watermarks are compared with the original one using Eqn. 21. Further, the attacked biometric template after above mentioned attacks are depicted in figure 3. The detailed results in order to verify robustness of the proposed scheme are discussed below.

The most common manipulation in digital images is filtering. The watermarked fingerprint image is filtered by average and median filtering considering 5×5 window and watermark is then extracted from the attacked images. The visual results are depicted in the figures 4(a) and (b) respectively. Another most common method to estimate the robustness of watermark is the addition of noise. In many cases, the degradation and distortion of the image are due to noise addition. Robustness against additive noise is estimated by degrading watermark fingerprint image by adding 25% Gaussian noise randomly. It is clear from the figure 3(c) that lot of information is lost after this attack but the extracted watermark (figure 4(c)) is well recognizable. To check the robustness against Image Compression, the watermarked fingerprint image is attacked by JPEG compression attack. The extracted watermark logo from compressed Watermarked fingerprint image using JPEG compression with compression ratio 50 is given in figure 4(d). Image cropping is another most common manipulation in digital images. To check the robustness against Image Cropping, 40% area of the watermarked fingerprint image is cropped and then watermark is extracted. The

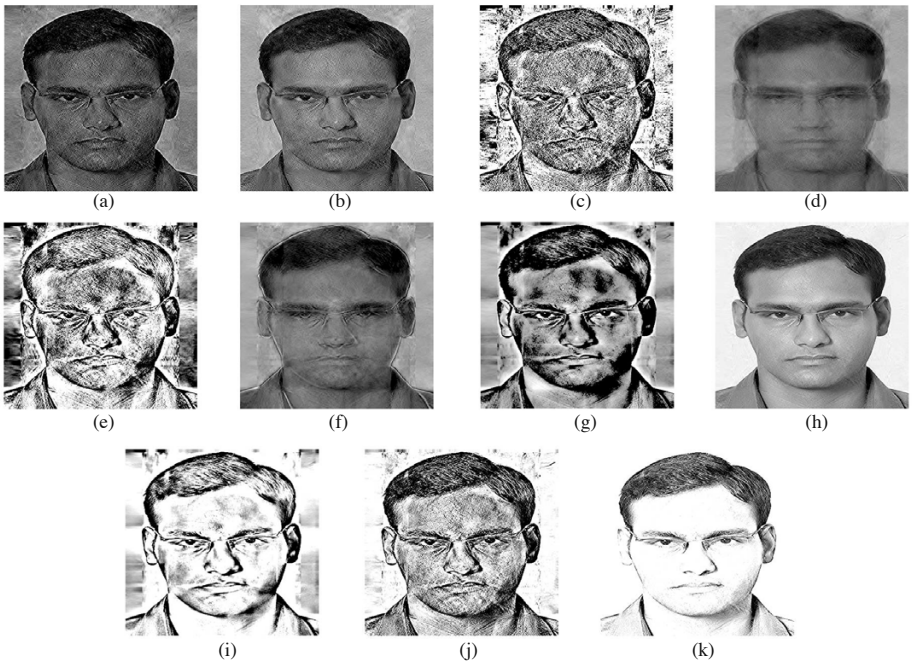

Figure 4: Extracted Watermark Image after a) Average Filtering (5×5) b) Median Filtering (5×5) c) Gaussian Noise Addition (25%) d) JPEG Compression (CR=50) e) Cropping (60% area remaining) f) Resizing ($388 \times 374 \rightarrow 256 \times 256 \rightarrow 388 \times 374$) g) Rotation (30°) h) Histogram Equalization i) Contrast Adjustment (Reduced by 50%) j) Contrast Adjustment (Increase by 50%) k) Sharpening (Increase by 50%).

corresponding visual results are given in figure 4(e). Enlargement or reduction is commonly performed to fit the image into the desired size resulting in information loss of the image including embedded watermarks. Hence, the proposed technique is also tested for resizing attack. For doing this task, the size of watermarked fingerprint image is first reduced to 256×256 and then carried back to its original size i.e. 388×374 followed by the watermark extraction and corresponding results are shown in figure 4(f). The proposed technique is also tested for rotation attack. For this purpose, the watermarked fingerprint image is rotated by 30° (see figure 4(g)). In figures 4(h), (i,j) and (k), the results for Histogram equalization, Contrast Adjustment and Sharpening attacks are shown respectively. For Contrast Adjustment, the contrast of the watermarked fingerprint image is decreased and increased by 50% whereas the sharpness of the watermarked image is increased by 50% for sharpening attack. The correlation coefficients of all extracted watermarks are depicted in table 1.

Table 1: Correlation Coefficients of Extracted Watermarks after Attacks.

Attacks	ρ	Attacks	ρ
No Attack	1	Resizing ($388 \times 374 \rightarrow 256 \times 256 \rightarrow 388 \times 374$)	0.9687
Average Filtering (5×5)	0.9403	Rotation (30°)	0.9187
Median Filtering (5×5)	0.9751	Histogram Equalization	0.9660
Gaussian Noise Addition (25%)	0.9780	Contrast Adjustment (50% decreased)	0.9577
JPEG Compression ($CR = 50$)	0.9720	Contrast Adjustment (50% decreased)	0.9987
Cropping (60% area remaining)	0.9178	Sharpening (50% increased)	0.9634

5. Conclusions

In this work, a novel scheme is presented to improve the security of biometric templates, in which diffusion and watermarking methods are combined to ensure the authenticity, confidentiality, and integrity of the templates. The diffusion is accomplished by non-linear chaotic map and Hessenberg decomposition. The use of chaotic map gives the randomness whereas Hessenberg decomposition makes the process invertible followed by the embedding of the watermark, which makes our system more secure and protected from different attacks. Furthermore, to evaluate the proposed system, we performed a series of experiments. The experimental results clearly demonstrate the improved performance in terms of imperceptibility and robustness against different kinds of attacks.

References

[1] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, Berlin, Germany, 2003.
[2] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K.V. Kumar, Biometric Encryption using Image Processing, in: Proc. Optical Security and Counterfeit Deterrence Techniques II, San Jose, CA, 3341, 1998, pp. 178–188.
[3] D. Moon, Y. Chung, S.B. Pan, K. Moon and K.I. Chung, An efficient selective encryption of fingerprint images for embedded processors, ETRI Journal, 28, 2006, pp. 444–452.
[4] I.J. Cox, Digital Watermarking, Morgan Kaufmann Publishers, CA, USA, 2002.
[5] G. Bhatnagar and B. Raman, A new robust Reference Watermarking Scheme based on DWT-SVD, Computer Standards and Interfaces, 31(5), 2009, pp. 1002–1013.
[6] G. Bhatnagar and B. Raman, Robust Reference Watermarking Scheme using Wavelet Packet Transform and Bidiagonal-Singular Value Decomposition, International Journal of Image and Graphics, 9(3), 2009, pp. 449–477.
[7] G. Bhatnagar and B. Raman, Distributed Multiresolution Discrete Fourier Transform and its Application to Watermarking, International Journal of Wavelet, Multiresolution and Information Processing, 8(2), 2010, pp. 225–241.
[8] S. Jain, Digital Watermarking Techniques: A Case Study in Fingerprints and Faces, Proc. Indian Conference on Computer Vision, Graphics and Image Processing, 2000, pp. 139–144.
[9] A.K. Jain, K. Nandakumar, and A. Nagar, Biometric Template Security, EURASIP Journal on Advances in Signal Processing, 2008, 2008, pp. 1–17.
[10] A.K. Jain and U. Uludag, Hiding Biometric Data, IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(11), 2003, pp. 1494–1498.
[11] B. Gunsel, U. Uludaga and A.M. Tekalp, Robust Watermarking of Fingerprint Images, Pattern Recognition, 35(12), 2002, pp. 2739–2747.
[12] A.K. Jain, U. Uludag and R. Hsu, Hiding a Face in a Fingerprint Image, Proc. International Conference on Pattern Recognition, 3(3), 2002, pp. 756–759.
[13] M. Yeung and S. Pankanti, Verification Watermarks on Fingerprint Recognition and Retrieval, Journal of Electronic Imaging, 9(4), 2000, pp. 468–476.
[14] U. Uludag, B. Gunsel, and M. Ballan, A spatial method for watermarking of fingerprint images, Proc. Intl. Workshop on Pattern Recognition in Information Systems, Setbal, Portugal, 2001, pp. 26-33.
[15] M. Pollicott and M. Yuri, Dynamical systems and ergodic theory, London Mathematical Society Student Text Series, Cambridge, 1998.
[16] S. Tao, W. Ruli and Y. Yixun. Generating Binary Bernoulli Sequences Based on a Class of Even-Symmetric Chaotic Maps, IEEE Trans. on Communications, 49(4), 2001, pp. 620–623.
[17] G.H. Golub and C.F.V. Loan, Matrix computations. Johns Hopkins University Press, 1996.
[18] `http://bias.csr.unibo.it/fvc2002/download.asp`